Accelerate Your Transition to SAP NS2's Secure HANA Cloud

Whitepaper - January 25, 2019

Table of Contents

OVERVIEW

The SAP National Security Services (NS2) Secure HANA Cloud (SHC) on Amazon Web Services (AWS) presents a comprehensive offering to the national security community that leverages enterprise scale support with cloud infrastructure designed to support both SAP and non-SAP solutions. The SHC offering on AWS utilizes the technical innovations presented by SAP and Amazon and integrates them directly into the infrastructure supporting the applications.

The SHC offering includes cloud infrastructure and Secure Cloud Delivery (SCD), a set of specialized NS2 remote resources that help manage the landscape and optimize SAP applications.

SCD provides the specialized resources to help on-board your landscape into AWS and optimize the transition with proven SAP expertise. Our offering is designed to augment your existing team and enable your journey into the cloud.

SHC incorporates SAP best practices with a secure cloud delivery model. Our intellectual property provides customers with a reference architecture designed to run SAP solutions for your industry on the hyperscaler of your choice. The challenge customer's encounter is that they do not possess the internal resources to securely provision their mission critical systems directly with an individual hyperscaler. SHC provides an automated and secure deployment model that natively incorporates the right controls, configurations and capacity requirements required to provision SAP solutions in the cloud. We also incorporate the necessary safeguards and cybersecurity procedures to help secure your information. SHC provides the necessary controls and capabilities to enable your digital transformation. Innovations such as machine learning, artificial intelligence and analytics are made available by the NS2 Cloud offerings.

As SHC securely provisions and deploys your digital assets across AWS GovCloud (US), the security safeguards are inherently apart of the build process. In addition, SHC leverages our team of remote SAP experts to securely patch and remediate vulnerabilities across the solution stack. This provides a secure layer that protects against hackers and other digital threats. We prioritize the preservation of our customer's data and we also offer a comprehensive high availability and/or disaster recovery strategy that safeguards our customer's data that is designed specifically for AWS infrastructure.

SHC RUNS ON AWS GOVCLOUD (US) INFRASTRUCTURE

AWS GovCloud (US) delivers a cloud platform built upon the foundational principles of security, privacy, control, compliance, and transparency. Public Sector entities receive physically isolated regions of Amazon Web Services that employ world-class security and compliance services critical to U.S. government entities for all systems and applications built on the architecture. These services include:

- FedRAMP High
- Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) for Impact Levels 2, 4 and 5
- DOJ's Criminal Justice Information Systems (CJIS) Security Policy
- U.S. International Traffic in Arms Regulations (ITAR)
- Export Administration Regulations (EAR)
- FIPS 140-2
- IRS-1075, and other compliance regimes.

The cloud community supports only US Federal, state, local, and tribal governments and their partners. SHC on AWS offers not only the support required to quickly and successfully deploy SAP workloads in the cloud, but the ability to scale elastically with your business requirements.

ACCELERATE YOUR TRANSITION TO THE CLOUD (SECURELY)

Deploying and running infrastructure on AWS GovCloud (US) has specific requirements for running SAP workloads. SHC makes it easier for customers to leverage the innovation from SAP and AWS because the offering was designed with one goal in mind:

- *To accelerate and optimize a customer's transition into the cloud*

Our team starts off by working with the customer to identify the required SAP reference architecture to run your SAP solutions. We perform the onboarding tasks to securely, effectively and efficiently setup the cloud landscape. Once built, our team manages the 24/7 steady state support across the life of the contract. This approach allows customers to overcome security risks, performance issues, and delayed timelines that often result when moving to the cloud.

PROVEN AND COMPLIANCE-DRIVEN ENTERPRISE LEVEL SECURITY

Our team provides security across the entire solution stack where we enable data encryption at rest and in transit. The following list provides insight into our security posture:

- Hardened Amazon Machine Images (AMIs) that adhere to the highest level of security standards.
- AWS Key Management Service (KMS), a FIPS 140-2 certified service which offers customers managed encryption keys in the AWS GovCloud (US).
- AWS EBS volume encryption, and S3 server-side encryption for data at rest encryption. SSL/TLS connections and IPSEC VPNs to encrypt data in transit.
- Virtual firewalls are also implemented using customer-defined access rules and have the ability to restrict traffic at the IP address and protocol level.
- A baseline set of security groups designed to run SAP solutions. These security groups protect the SAP application and also incorporate the necessary firewall rules to secure the application stack.
- We help implement the customer's firewall rules into the solution to comply and support the security policy of each customer.
- Instances that are assigned to one or more security groups and the associated firewall rules allow traffic to or from its associated system.
- The SCD team implements the necessary Network Access Control Lists (NACL) to enable the different Virtual Provide Clouds (VPCs) to communicate in order for the SAP solution to work as required. This security capability acts as a high-level firewall for controlling the traffic in and out of the VPC.

SHC provides these catered security services in our overall subscription. Without SHC, customers need to create, configure and implement the security tools on their own. A manual implementation of the security tools may impact the SAP solutions and degrade performance of the applications in the cloud. SHC mitigates these risks and offers a proven and compliance-based methodology for securely provisioning SAP workloads on AWS.

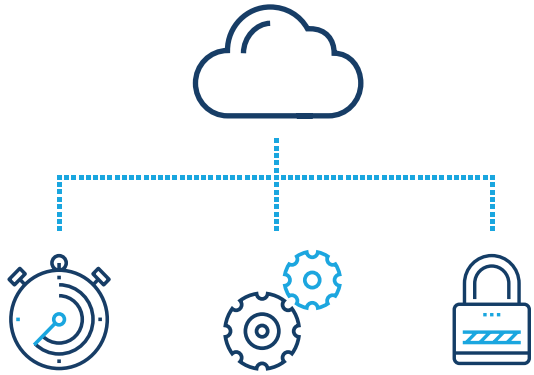
APPLICATION SERVICE LEVEL AGREEMENT (SLA)

In addition, our solution provides service levels that are relevant to the business community. SHC on AWS provides customers a service level agreement (SLA) that measure the uptime of the SAP application. If the solution is up and running then we are meeting our objectives for our customers. This is a different philosophy than other cloud providers. Most cloud providers only provide SLAs that relate to the uptime of the infrastructure. In these instances, virtual machines could be running successfully but the applications are down. For most cloud providers, the customer would not receive any credit on their bill and they still would have downtime issues that would need to be resolved on their own accord.

The SHC provides this level of performance because our customers deserve the highest standard of support and performance. Their investment in our solution requires our highest commitment to the customer and our standard of excellence is measured by the SLAs that we incorporate in our solution.

AUTOMATION (WITH EXPERIENCE COMES KNOWLEDGE)

SHC is designed to lower cost and accelerate the cloud deployment and production go-live. It achieves this by leveraging purpose-built processes and automation based on our experiences with Government and Regulated Industries. These predefined processes are created, managed and deployed by SAP NS2's Secure Cloud Delivery (SCD) team. Working with the customer, the SCD team ensures that all instances are provisioned and connected to the secure cloud environment.



Our team consists of U.S. persons on U.S. soil who have a deep knowledge and understanding of SAP applications, AWS GovCloud (US) services and our proven cloud delivery methods. We are responsible for infrastructure, networking, operating system, database support and technical application support. We also work alongside AWS to provide our customer with the necessary management and maintenance of the different servers, storage, and network devices as necessary.

The value to our customers is that we provide this expertise throughout the life of the contract and it is designed to supplement the existing resources from the customer We provide our customers cloud infrastructure and world class support across their application portfolio.

NS2 NATIONAL SECURITY SERVICES

877-972-7672
info@sapns2.com
www.sapns2.com

Now, let us help you. Learn more at sapns2.com/capabilities/ns2-cloud/